NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC-015/88
19 February 1988

MEMORANDUM FOR THE MEMBERS, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

SUBJECT: Proposed "National Policy for Granting Access to U.S. Classified Cryptographic Information" -- **ACTION MEMORANDUM**

1. As directed by the Acting Chairman during the 17 February Committee meeting, the enclosed subject policy proposal is provided for vote by the membership. This version of the policy reflects changes which the members indicated as being acceptable. Please return the accompanying vote sheet (Enclosure 3) to the NTISSC Secretariat **by 24 March 1988.**

2. For your convenience, a summary of the changes is at Enclosure 1; changes are highlighted by an asterisk (*) in the right hand margin of the draft.

STAT

Executive Secretary

3 Encls:
a/s

cc: Observers to the NTISSC

NATIONAL POLICY FOR GRANTING ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

SECTION I - POLICY

1. Certain U.S. classified cryptographic information, the loss of which could cause serious or exceptionally grave damage to U.S. national security, requires special access controls. Accordingly, this policy establishes a formal cryptographic access program whereby access to certain U.S. classified cryptographic information shall only be granted to individuals who satisfy the criteria set forth herein.

SECTION II - DEFINITION

2. As used in this policy, U.S. classified cryptographic information is defined as:

a. TOP SECRET and SECRET, CRYPTO designated, key and authenticators.

b. All cryptographic media which embody, describe, or implement classified cryptographic logic; this includes full maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, cryptographic computer software, or any other media which may be specifically identified by the National Telecommunications and Information Systems Security Committee (NTISSC). * *

SECTION III - CRITERIA

3. An individual may be granted access to U.S. classified cryptographic information, only if that individual:

a. Is a U.S. citizen;

b. Is an employee of the U.S. Government, is a U.S. Government contractor or employee of such contractor, or is employed as a U.S. Government representative (including consultants of the U.S. Government);

c. Requires access to perform official duties for, or on behalf of, the U.S. Government;

d. Possesses a security clearance appropriate to the classification of the U.S. cryptographic information to be accessed;

e. Possesses a valid need-to-know for the information;

SUMMARY OF CHANGES

1. Second paragraph of the FOREWORD -- in the second sentence (third line), the phrase "...polygraph need not..." now reads "polygraph is not intended to...". Also, the last sentence of this paragraph which read "Rather, it is intended that each department and agency utilize the potential deterrent factor of the polygraph as it deems necessary and at its own discretion" has been deleted.

2. First page of the policy, SECTION II - DEFINITION, the last line of paragraph 2.b. -- "National Manager" has been replaced with "National Telecommunications and Information Systems Security Committee (NTISSC)".

3. Page 2 of the policy, paragraph 3.h.:

a. (First line) the words "Voluntarily consents to..." have been replaced by "Acknowledges that he/she may...";

b. Additionally, the words "which shall be" that previously appeared on line three of paragraph 3.h. between the words "examination" and "administered", have been stricken.

c. The last sentence of this paragraph ("The examining official shall only select questions which concern espionage, sabotage, or questions which relate to the unauthorized disclosure of U.S. classified cryptographic information.") has been deleted.

4. Page 3 of the policy, paragraph 6.e. has been deleted. (Paragraph read: "Accept, as valid, Cryptographic Access Certificates granted by other federal departments and agencies.")

As a result, subparagraph f. is now subparagraph e.

5. Annex A, page A-1, fifth paragraph -- in the first sentence (second line) the phrase "...you must voluntarily consent to...", now reads: "...you must acknowledge the possibility that you may...".

6. Annex A, page A-2, first paragraph -- in the first sentence (first line) the phrase "...to be subject to...", now reads: "to accept the possibility of being subject to...". Additionally, in the second sentence (line six), the words "a consent" have been replaced with the words "an acknowledgement".

7. Annex B, page B-1, paragraph b. -- fourth sentence (lines 10 and 11), the phrase "I voluntarily consent to..." now reads: "I acknowledge that I may...".

Enclosure 1

19 February 1988

NTISS
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

NATIONAL POLICY

FOR

GRANTING ACCESS TO U.S. CLASSIFIED

CRYPTOGRAPHIC INFORMATION

nclosure 2

DRAFT

FOREWORD

Pursuant to the authority of Executive Order 12333 and National Security Decision Directive 145, and in accordance with Executive Order 12356, Section 4.2, there is hereby established a program governing access to U.S. classified cryptographic information. It is recognized that the technically sophisticated cryptographic systems employed by the United States Government can be compromised if the human element is not subject to certain reasonable controls regarding access to the U.S. classified cryptographic information supporting these systems. Therefore, NTISSP No. XXXX was developed by the National Telecommunications and Information Systems Security Committee (NTISSC) for the purpose of reinstating formal cryptographic access as a means of preventing loss or unauthorized disclosure of U.S. classified cryptographic information.

Within the scope of this policy, reference is made to the use of the non-lifestyle, counterintelligence scope polygraph examination. It should be noted that the polygraph is not intended to be used as a prescreening mechanism for determining cryptographic access. * * * *

NOTE: Modifications to the previous version of the draft policy are indicated by an asterisk (*).

DRAFT

f. Receives a security briefing appropriate to the U.S. classified cryptographic information to be accessed;

g. Acknowledges the granting of access by signing a Cryptographic Access Certificate; and

h. Acknowledges that he/she may be subject to a non-lifestyle, counterintelligence scope polygraph examination administered in accordance with department or agency directives and applicable law. *

4. All persons indoctrinated for cryptographic access within the guidelines of this program must comply with requirements, prescribed in department or agency security directives, regarding unofficial foreign travel or contacts with foreign nationals.

SECTION IV - APPLICATION

5. This policy shall apply to all individuals who are required to have access to U.S. classified cryptographic information in the performance of their normal duties. Accordingly, the provisions of this policy apply to those individuals assigned:

a. As COMSEC custodians or alternates.

b. As producers or developers of cryptographic key or logic.

c. As cryptographic maintenance or installation technicians.

d. To facilities where cryptographic keying materials are generated or stored.

e. To prepare, authenticate, or decode valid or exercise nuclear control orders.

f. In secure telecommunications facilities located in fixed ground facilities or on board ships.

g. Any other responsibility with access to U.S. classified cryptographic information which is specifically identified by the head of a department or agency.

SECTION V - RESPONSIBILITIES

6. The heads of federal departments and agencies shall:

a. Implement the provisions of this policy within their respective department or agency.

b. Ensure that a capability exists within the department or agency to obtain the resources necessary to administer any polygraph examinations. This may be accomplished either by directly programming and funding for these resources or by executing agreements or arrangements to utilize the existing resources of another department or agency.

c. Develop and administer a "Cryptographic Access Briefing" which shall address the specific security concerns of the department or agency; an example of such a briefing is presented in Annex A.

d. Prepare a "Cryptographic Access Certificate" which shall be signed by all individuals granted cryptographic access in accordance with this program; an example of such a certificate is presented in Annex B. The Cryptographic Access Certificate shall be made a permanent part of the individual's official security records and shall be accounted for in accordance with department or agency directives concerning retention of security clearance/access certificates.

e. Ensure that applicable department or agency security directives contain requirements for reporting unofficial foreign travel and contacts with foreign nationals. * * * *

SECTION VI - EXCEPTIONS

7. Exceptions to this policy may be approved by department or agency heads to meet exigent operational needs. Records of exceptions granted shall be made available to the National Manager on request.

2 Encls:

1. Annex A, Cryptographic Access Briefing (SAMPLE)
2. Annex B, Cryptographic Access Certificate (SAMPLE)

SAMPLE

CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to U.S. classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect U.S. classified cryptographic information. You must understand the directives which require these safeguards and the penalties you will incur for willful disclosure of this information to unauthorized persons.

U.S. classified cryptographic information is especially sensitive because it is used to protect classified information which relates to our national security. Disclosure of this information to unauthorized persons, could result in irreparable damage to the United States. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on U.S. classified cryptographic information are a necessary component of government programs to ensure that our Nation's vital secrets are not compromised.

Because access to U.S. classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, department or agency implementing directives covering the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

Especially important to the protection of U.S. classified cryptographic information is the timely reporting of any known or suspected compromise of this information. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

As a condition of access to U.S. classified cryptographic information, you must acknowledge the possibility that you may be subject to a non-lifestyle, counterintelligence scope polygraph examination. This examination will be administered in accordance with the provisions of (insert appropriate department or agency directive) and applicable law. This polygraph examination will only encompass questions concerning espionage, sabotage, or

DRAFT

questions relating to unauthorized disclosure of classified information.

You have the right to refuse to accept the possibilty of being subject to a non-lifestyle, counterintelligence scope polygraph examination. Such refusal will not be cause for adverse action but may result in your being denied access to U.S. classified cryptographic information. If you do not, at this time, wish to sign such an acknowledgement as a part of executing the Cryptographic Access Certificate, this briefing will be terminated at this point and the briefing administrator will so notate the Cryptographic Access Certificate.

* * * * * * * * * * * * * * * * * * * *

You should know that intelligence services of some foreign governments prize the acquisition of U.S. classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge U.S. classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, U.S. classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to gain knowledge regarding the U.S. classified cryptographic information you have must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to certain communist or other designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

Finally, you must know that, should you willfully disclose to any unauthorized persons any of the U.S. classified cryptographic information to which you will have access, you may be subject to administrative and personnel security actions as well as prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States.

CRYPTOGRAPHIC ACCESS CERTIFICATE

INSTRUCTION

Section I of this certificate must be executed before an individual may be granted access to U.S. classified cryptographic information. Section II will be executed when the individual no longer requires such access. This certificate (original) will be made a permanent part of the official security records of the individual concerned.

SECTION I

AUTHORIZATION FOR ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

a. I understand that I am being granted access to U.S. classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.

b. I understand that safeguarding U.S. classified cryptographic information is of the utmost importance and that the loss or compromise of such information could lead to irreparable damage to the United States. I understand that I am obligated to protect U.S. classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my security office, regarding unofficial foreign travel or contacts with foreign nationals. I acknowledge that * I may be subject to a non-lifestyle, counterintelligence * scope polygraph examination to be administered in accordance with (insert appropriate department or agency directive) and applicable law.

c. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the UCMJ and/or the criminal laws of the United States. I understand and accept that unless

I am released in writing by an authorized representative of (insert appropriate security office) the terms of this certificate and my obligation to protect all U.S. classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

ACCESS GRANTED THIS DAY OF 19

SIGNATURE NAME/GRADE,RANK,RATING/SSN

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION

SECTION II

TERMINATION OF ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to U.S. classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any U.S. classified cryptographic information I acquired, nor discuss with any person any of the U.S. classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).

ACCESS WITHDRAWN THIS DAY OF 19

SIGNATURE NAME/GRADE, RANK, RATING/SSN

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION

DRAFT

PRIVACY ACT STATEMENT

Authority to request Social Security Number (SSN) is Executive Order 9397. Routine and sole use of the SSN is to identify the individual precisely when necessary to certify access to U.S. classified cryptographic information. While disclosure of your SSN is voluntary, failure to do so may delay certification and in some cases, prevent original access to U.S. classified cryptographic information.

SIGNATURE DATE

NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

NTISSC-015/88

MY VOTE ON NTISSC-015/88

IS AS FOLLOWS:

CONCUR: _____

NON-CONCUR: _____

ABSTAIN: _____

_____
(SIGNATURE)

_____
(TITLE)

_____
(AGENCY/DEPARTMENT)

_____
(DATE)

After indicating your vote, please sign, date and return this sheet to:

Executive Secretary, NTISSC
Ops Bldg #3, Room COW89
National Security Agency
Ft. George G. Meade, MD. 20755-6000

Phone: 688-7355/688-7736

Enclosure 3